REPORT OF
MARKET CONDUCT EXAMINATION
OF

PENNSYLVANIA PROFESSIONAL LIABILITY JOINT UNDERWRITING ASSOCIATION

Plymouth Meeting, Pennsylvania

AS OF
August 16, 2005

COMMONWEALTH OF PENNSYLVANIA

INSURANCE DEPARTMENT
MARKET CONDUCT DIVISION

Issued: October 4, 2005

VERIFICATION

Having been duly sworn, I hereby verify that the statements made in the within document are true and correct to the best of my knowledge, information and belief. I understand that false statements made herein are subject to the penalties of 18 Pa. C.S. §4903 (relating to false swearing).

Lawrence R. Lentini, CPA
President, INS Services, Inc.

Sworn to and Subscribed Before me

This 9th Day of August, 2005

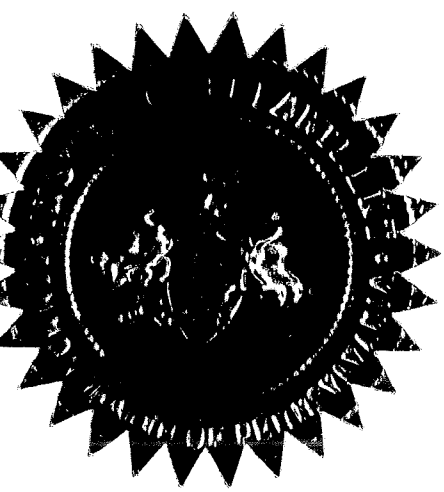
Notary Public

NOTARIAL SEAL
CHRISTINE A. HAGGERTY, Notary Public
City of Philadelphia, Phila. County
My Commission Expires July 2, 2006

BEFORE THE INSURANCE COMMISSIONER
OF THE
COMMONWEALTH OF PENNSYLVANIA

ORDER

AND NOW, this 29 day of April, 2002, in accordance with Section 905(c) of the Pennsylvania Insurance Department Act, Act of May 17, 1921, P.L. 789, as amended, P.S. § 323.5, I hereby designate Randolph L. Rohrbaugh, Deputy Insurance Commissioner, to consider and review all documents relating to the market conduct examination of any company and person who is the subject of a market conduct examination and to have all powers set forth in said statute including the power to enter an Order based on the review of said documents. This designation of authority shall continue in effect until otherwise terminated by a later Order of the Insurance Commissioner.



M. Diane Koken
Insurance Commissioner

Pennsylvania Professional Liability
Joint Underwriting Association

Docket No.
MC05-10-006

Market Conduct Examination as
of the close of business on August 16, 2005

ORDER

A market conduct examination of Pennsylvania Professional Liability Joint Underwriting Association (referred to herein as "Respondent") was conducted in accordance with Article IX of the Insurance Department Act, 40 P.S. §323.1, et seq., for the period May 1, 2005 through August 16, 2005. The Market Conduct Examination Report disclosed exceptions to acceptable company operations and management practices. Based on the documentation and information submitted by the Respondent, the Department is satisfied that the Respondent will take corrective measures pursuant to the recommendations of the Examination Report.

It is hereby ordered as follows:

1. The attached modified Examination Report will be adopted and filed as an official record of this Department. All findings and conclusions resulting from the review of the Examination Report and related documents are contained in the attached Examination Report.

2. Respondent shall comply with Pennsylvania statutes and regulations.

3. Respondent shall comply with all recommendations contained in the attached Report.

4. Respondent shall file an affidavit stating under oath that it will provide each of its directors, at the next scheduled directors meeting, a copy of the adopted Report and related Orders. Such affidavit shall be submitted within thirty (30) days of the date of this Order.

The Department, pursuant to Section 905(e)(1) of the Insurance Department Act (40 P.S. §323.5), will continue to hold the content of the Examination Report as private and confidential information for a period of thirty (30) days from the date of this Order.

BY: Insurance Department of the Commonwealth
of Pennsylvania

_____ (October 4, 2005)
Randolph L. Rohrbaugh
Deputy Insurance Commissioner

INS SERVICES, INC.

Insurance Regulatory Services

New Market
Suite 306
419 So. 2nd Street
Philadelphia, PA 19147
Phone: (215) 625-8642
Fax: (215) 625-9494

April 7, 2005

Mr. Dennis C. Shoop
Commonwealth of Pennsylvania
Insurance Department
Director, Bureau of Enforcement
1321 Strawberry Square
Harrisburg, PA 17120

Re: **Pennsylvania Professional Liability Joint Underwriting Association**

According to the terms of an Engagement Letter dated February 3, 2005 and entered into by the Pennsylvania Insurance Department (the Department) and INS Services, Inc., whereby INS Services, Inc. was retained to perform certain services related to a market conduct examination of Pennsylvania Professional Liability Joint Underwriting Association (the JUA) pursuant to Article IX of the Insurance Department Act of May 7, 1921, P.L. 789, No. 285, added December 18, 1992, P.L. No. 177 (40 P.S. §323.1-323.8), this report addresses the following issues related to that examination:

1. Review and evaluation of JUA management practices,

2. Evaluation of JUA underwriting and claims practices and operations, and

3. Evaluation of internal control structures relating to claims management and policy issuance.

Background

The JUA is a nonprofit, unincorporated association created by Article VIII of the Pennsylvania Health Care Services Malpractice Act, effective January 13, 1976. The purpose of the JUA is to ensure that all health care providers within

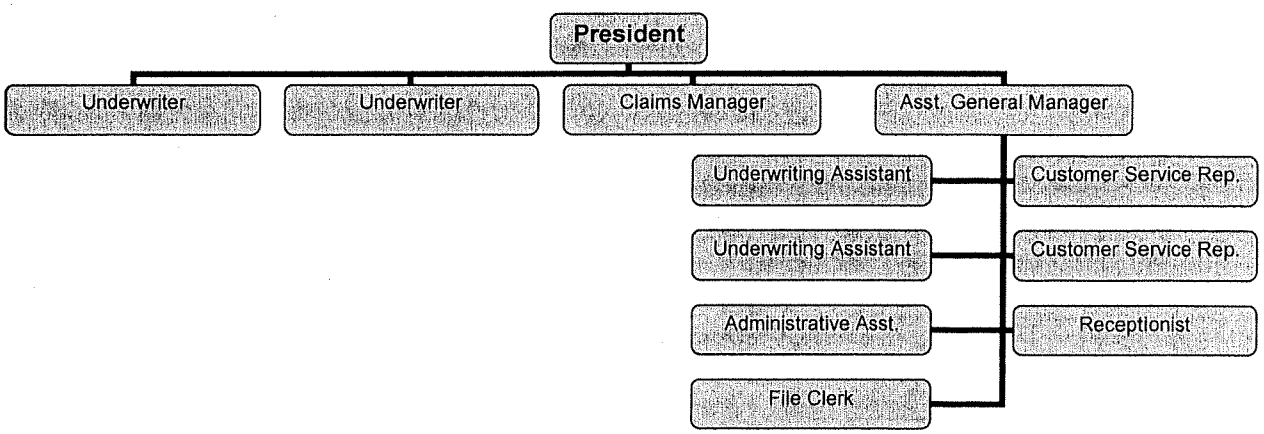
Pennsylvania are afforded access to malpractice insurance on reasonable and not unfairly discriminatory terms. The JUA writes medical malpractice insurance for medical practitioners and health care institutions that cannot conveniently and expeditiously obtain such insurance coverage in the commercial marketplace.

Commonly known as the "market of last resort" for medical liability insurance, the JUA typically provides professional medical liability insurance for health care providers who cannot obtain insurance from other licensed or approved insurers, for reasons not attributable to neglect, oversight or willfulness in failing to obtain insurance for periods for which coverage was otherwise available. The JUA also provides insurance for health care providers who become uninsured as a result of insolvency of insurers previously licensed or otherwise approved to provide such insurance with the Commonwealth of Pennsylvania.

The JUA provides primary insurance coverage on a claims-made basis for institutions and practitioners who previously had coverage on a claims-made basis. Occurrence based coverage is also available for health care providers who previously had coverage on an uninterrupted occurrence basis. Policy forms, rates, rating plans, rating rules and rating classifications must be filed and approved by the Department. Rates are determined by the JUA's consulting actuaries and approved by the Department and are based on the JUA's and other admitted carrier's loss and expense experience.

Organizational Structure

The JUA currently employs twelve to fifteen employees generally organized in a traditional structure as shown on the chart below.



Overall, the JUA's organizational structure of tasks and authority relationships are well designed so work is accomplished at a high level of

performance. Job content, duties, methods and relationships are clearly documented to satisfy both organizational and individual requirements.

The JUA maintains a comprehensive Employee Handbook describing personnel policy and procedures. The Employee Handbook serves as a working guide for management and staff personnel in the day-to-day administration of the JUA's personnel program. Management also maintains a Procedure Manual containing a detailed description of the JUA procedures and practices. A useful Procedure Task Level Guide is available as well to describe various JUA tasks, level of expertise required by task and the individuals with primary and secondary job responsibility for each task.

External Environment

The medical professional liability market for practitioners and health care institutions can be very cyclical. At the peak of a market cycle, insurance rates begin to catch up with underwriting experience, insurance carriers come back into the market to write health care liability policies and provider-owned mutual insurance companies are created. In this environment, the market gradually recovers; competition comes alive while availability and affordability are much less of an issue.

In the trough of a market cycle when rates have not kept pace with liability exposure, the insurance marketplace dries up. Medical liability insurers in the Commonwealth withdraw or cut-back in writing health care exposures in response to a period of excessive judgments and defense costs affecting hospitals, physicians, and other allied health care professionals. Given this environment, the availability and affordability of health care liability insurance becomes a serious concern.

These uncontrollable external market forces present hard judgment calls for management of the JUA. On one hand, the JUA must incur costs to streamline procedures, acquire new hardware and software, and provide for staff training to be prepared for a potential higher number of medical practitioners and health care institutions in need of liability insurance if capital to support professional liability insurance in the Commonwealth shrinks. Yet on the other hand, the JUA can effectively hold down current operating expenses by maintaining the status quo whereby the JUA runs smoothly to provide professional liability insurance at current levels of activity. The JUA's external environment presents conditions for hard judgment calls that require thoughtful study and analysis.

1 - Management Practices

The importance of effective leadership for obtaining individual, group, and organizational performance is critical. Since April, 2001, Susan Sersha has held the position of President of the JUA. Ms. Sersha is an experienced insurance executive. She possesses the knowledge, experience and demonstrated leadership skills to effectively lead the JUA's current level of activity. She has also demonstrated leadership skills to spearhead a response to an unexpected increase in policyholders caused by external forces beyond the control of the JUA.

Ms. Sersha also serves as a manager in close, day-to-day contact with JUA staff members. This activity is highly interpersonal but apparently efficient and effective, given the small number of employees. In the event the JUA grew rapidly, the hands-on management style could become less effective, depending on the volume of that growth, and whether it is sustained growth, or just temporary and isolated.

Additional mitigating factors include her sharing of certain senior management responsibilities with Rick Lambrecht who joined the JUA in June 2003 to serve as Assistant General Manager, and Nancy McKittrick, Claims Manager. Mr. Lambrecht is an experienced insurance claims manager with substantial practical experience primarily as a claims supervisor with several insurance companies. He has become familiar with most JUA job functions, so he could temporarily absorb an unexpected workload in several capacities in the event a need arose.

At times, Ms. McKittrick also handles some financial functions as well as HIPPA training and vendor contact. She works closely with the actuaries on several matters and would be able to assist with the financial statements should the need arise.

Ms. Sersha's leadership style promotes confidence and trust with staff members. Staff members feel free to discuss job problems with Ms. Sersha or Mr. Lambrecht, who in turn solicit staff member ideas and opinions. This interaction in a relatively small organization efficiently promotes a team environment to effect the JUA's methods and goals.

Outsourced Services and Operating Arrangements

In the event a company licensed or approved to write professional liability insurance business in Pennsylvania withdrew from the market or otherwise faced financial difficulties, the JUA's outsourced service vendors most likely would have the capability to accommodate higher levels of activity until management had time

to make structural changes as circumstances warranted. The JUA has services and operating agreements in place with the following organizations.

- The Pennsylvania Fair Plan provides premium statistics, customer tracking and related information services.
- Accounting records are prepared by Blumenthal & Palmer, P.C.
- Auditors are PricewaterhouseCoopers, LLP.
- PrimePay Greater Philadelphia, Inc. processes payroll and payroll taxes.
- The JUA retains the services of Milliman Inc. to provide loss and loss expense reserve actuarial analysis.
- Deutsche Asset Management provides investment management services.
- The JUA uses the services of Pinnacle Risk Management to provide claims services for most claims reported to the JUA after January 1, 2003. Pinnacle's functions include claim processing, adjusting and legal expenses incurred in the claim adjusting process.

The following market conduct standards were evaluated:

Standard 1

The Company has an up-to-date, valid internal, or external audit program.

Comments: This standard does not have a direct statutory requirement. A Company that has no internal audit function lacks the ready means to detect structural problems until after problems have occurred. A valid internal or external audit function and its use is a key indicator of competency of management, which the Commissioner may consider in the review of an insurer.

Results: Pass

Observations: No formal internal audit program exists. However, monthly and quarterly reporting is reviewed by the Board of Directors, confirming an ongoing effort to track and study market conditions. Projections are also constructed as a basis for contingency planning. Also, the narrow business objectives of the organization limit the risk from changing market conditions. That is, competitive position is not an issue.

A financial audit is conducted annually by PricewaterhouseCoopers.

Recommendations: None

Standard 2

The Company has appropriate controls, safeguards and procedures for protecting the integrity of computer information.

Comments: This standard does not have a direct statutory requirement; however maintaining appropriate safeguards for protecting the integrity of the computer information is a public protection issue. Appropriate controls, safeguards and procedures for protecting the integrity of computer files are indicators of management competency which must be considered in the review of an insurer. Inherently, all computer hardware should be secured; data protected from unauthorized access; and routine backup procedures should mitigate risks of data loss or corruption.

Results: Failed, as related to physical data security

Observations: Policy and claim data is maintained on a Microsoft Windows 2000 network with domain level security. Passwords are required to access the domain and all data stored on the server, including financial and business data. Physical security however is lax. There are multiple entrances to the office, which remain unlocked and, at times unmonitored during business hours (8:00 AM until 4:30 PM). Occasionally, doors may remain unlocked and unmonitored even beyond business hours. The servers are in open office spaces. Tapes are kept on an open shelf. There is no archival service in use. Data is backed up daily and databases are replicated every two hours through the use of a batch routine. However, backup and disaster recovery procedures are not documented.

Externally, the JUA does not share protected health information with anyone except:

- Persons who legally represent the member
- Health Care Providers, who are required by the Health Care Portability & Accountability Act (HIPAA) to keep Protected Health Information confidential
- Business Associates with whom they have contractual agreements requiring that Protected Health Information be kept confidential
- Self-insured accounts, who are covered entities under HIPAA and held to its rules for confidentiality

Recommendations: Management should institute a broad security program to address physical and logical data security. Computer hardware and media should be kept in secure, environmentally safe areas. All security policies and procedures should be documented in detail and periodically tested for effectiveness.

Standard 3

The Company has antifraud initiatives in place that are reasonably calculated to detect, prosecute, and prevent fraudulent insurance acts.

Comments: Written procedural manuals or guides and antifraud plans should provide sufficient detail to enable employees to perform their functions in accordance with the goals and direction of management. Appropriate antifraud activity is important for asset protection as well as policyholder protection and is an indicator of competency of management, which the Commissioner may consider in the review of an insurer. Due to the statutory limitations on the organization, insurance fraud would generally be limited to obtaining coverage through the JUA without meeting the policy criteria, as well as risks stemming from employee dishonesty or breach of trust. Under 18 U.S.C. §1033, the JUA is required to report criminal actions to the Department.

Results: Failed.

Observations: The Employee Manual addresses conflicts of interest. The vast majority of claims are in litigation, so fraudulent activities are subject to numerous levels of review, both internal and external. Policyholders are advised of regulations via the JUA website and throughout the application process.

Recommendations: Establish a policy requiring employee criminal background checks.

Standard 4

The Company has a valid disaster recovery plan.

Comments: This standard does not have a direct statutory requirement; however the standard is inferred by broadly recognized best practices. It is essential that the Company have a formalized disaster recovery plan that will detail procedures for continuing operations in the event of any type of disaster. Appropriate disaster recovery planning is an indicator of competency of management that the Commissioner may consider in the review of an insurer.

Results: Fail

Observations: The Company has no formal Disaster Recovery Plan and no recovery testing has been conducted to date. While the JUA keeps backup copies of all server files, there is no secure off-site storage.

Recommendations: The disaster recovery plan should address items such as, but not limited to, environmental problems, hardware and software failures, sabotage

or any event that significantly disrupts normal data processing. The plan should be kept current, and readily available to appropriate personnel. The plan should include a list of key internal employees and all third party vendors that would assist in a disaster recovery effort. The plan should also be tested annually and modified based on the results of such tests.

Standard 5

The company adequately monitors the activities of the Managing General Agents (MGA).

No testing conducted, as this Standard is inapplicable.

Standard 6

Company contracts with MGA's comply with applicable statutes, rules and regulations.

No testing conducted, as this Standard is inapplicable.

Standard 7

Records are adequate, accessible, consistent and orderly and comply with state record retention requirements.

Comments: This standard is inferred from related statutes and outlined in "Guidelines for Record Retention", [30 Pa.B. 2968]. This standard is intended to assure that an adequate and accessible record exists for Company's transactions. The focus is on the records and actions considered in a market conduct examination such as, trade practices, claim practices, policy selection and issuance, rating, complaint handling, etc. Inadequate, disorderly, inconsistent, and inaccessible records can lead to inappropriate handling of claims, inappropriate rates and other issues that can harm the public.

Results: Pass

Observations: Management stated that all records are kept in accordance with statutory regulations. Iron Mountain stores all archived documents off-site and records are kept of storage dates and locations. The offsite storage records, maintained by JUA staff were provided and found adequate, although no material testing was performed.

Recommendations: None

Standard 8

The Company is licensed for the lines of business that are being written.

Comments: This standard, which deals with appropriate license to write policies, is less critical since the JUA was established by the Pennsylvania legislature.
Results: Pass.

Observations: The Joint Underwriting Association is authorized to write professional liability insurance by Pennsylvania statute. As evidenced by Subchapter C of Chapter 7 of Act 13 which "...establishes a nonprofit joint underwriting association to be known as the "Pennsylvania Professional Liability Joint Underwriting Association." Section 731, authorizes the Joint Underwriters Association to:"...Offer medical professional liability insurance to health care providers in accordance with section 732.""

Recommendations: None

Standard 9

The Company cooperates on a timely basis with examiners performing the examinations.

Comments: This standard has a direct insurance statutory requirement. The standard is aimed at assuring that the Company is cooperating with the Commonwealth in the completion of an open and cogent review of the Company's operations in Pennsylvania. Cooperation with examiners in the conduct of an examination is not only required by statute, it is conducive to completing the examination in a timely fashion and minimizing cost. Review methodology for this standard is based on response to all portions of the examination.

Results: Pass

Observations: The Company was able to provide requested information (when it existed) in a timely manner. Most follow-up questions were responded to immediately.

Recommendations: None.

Standard 10

The Company has procedures for the collection, use, and disclosure of information gathered in connection with insurance transactions so as to minimize any improper intrusion into the privacy of applicants and policyholders.

Comments: This standard has a direct insurance statutory requirement. The standard is intended to assure that the JUA provides adequate protection for

information it holds concerning its policyholders and minimizes any improper intrusion into the privacy of applicants, policyholders and claimants. Review methodology for this standard is by "generic" review. It is recognized that for the JUA, the policyholders are physicians who are also bound to HIPAA compliance in all aspects of patient record handling.

Results: Fail

Observations: The Company's facilities are not well protected from unauthorized access, as required by HIPAA (§ 164.306; 164.308; 164.310). File cabinets are readily accessible to anyone entering the office with or without approval. As noted elsewhere, physical security is lacking.

However, policies and procedures have been developed and/or defined in response to HIPAA privacy expectations and are readily available to all employees via a special privacy section on the Company's intranet. Employees are informed and sign off on confidentiality agreements. Archives of all inactive policy and claim information are securely stored off-site (Iron Mountain).

Recommendations: Employee access to paper and electronic information should be limited to specific individuals based upon need, and secured to prevent unauthorized access to personal healthcare information. Physical security should be enhanced to limit unauthorized access to information.

Standard 11

The Company has developed and implemented written policies, standards and procedures for the management of insurance information.

Comments: This standard has a direct insurance statutory requirement. The standard is intended to assure that the Company provides adequate protection for information it holds concerning its policyholders and minimizes any improper intrusion into the privacy of applicants and policyholders.

Results: Pass

Observations: As disclosed during interviews and as evidenced by the existence of the forms, employees are informed of the proper handling of personal information, and are required to sign-off on confidentiality and HIPAA compliance awareness. As disclosed in an interview with the president, few personal healthcare records are maintained by the JUA, as the organization is not involved in individual policies.

Recommendations: None

Standard 12

The Company has policies and procedures to protect the privacy of nonpublic personal information relating to its customers, former customers and consumers that are not customers.

No testing conducted, as the JUA only writes professional liability insurance and does not collect patient financial information. Thus, this standard is not applicable. HIPPA applies only to the extent of data regarding patient information included in the claim files. Further, substantial patient claim information is kept by the JUA's third party administrator. Lastly, the vast majority of claims involve filed lawsuits which are a matter of public record.

Standard 13

The Company provides privacy notices to its customers and, if applicable, to its consumers who are not customers regarding treatment of nonpublic personal financial information.

Comments: This standard has a direct insurance statutory requirement from the Pennsylvania Insurance Department by Chapter 146c of Title 31 which addresses the sharing of personal non-public financial information. As the JUA only writes professional liability insurance and does not collect patient financial information, for the most part, this standard is not applicable.

Results: Pass

Observations: The JUA does not handle, share or retain personal financial information of policyholders and patients. The only personal financial information the JUA receives relates to personal bankruptcy of claimants.

Recommendations: None.

Standard 14

If the Company discloses information subject to an opt out right, the Company has policies and procedures in place so that nonpublic personal financial information will not be disclosed when a consumer who is not a customer has opted out, and the Company provides opt out notices to its customers and other affected consumers.

Comments: This standard has a direct insurance statutory requirement from the Pennsylvania Insurance Department by Chapter 146c of Title 31 which addresses the sharing of personal non-public financial information. As the JUA only writes

professional liability insurance and does not collect patient financial information, this standard is not applicable.

Results: Pass

Observations: The JUA does not handle, share or retain personal financial information of policyholders and patients.

Recommendations: None.

Standard 15

The Company's collection, use and disclosure of nonpublic personal financial information are in compliance with applicable statutes, rules and regulations.

No testing conducted, as the JUA only writes professional liability insurance and does not handle, share or retain personal financial information of policyholders and patients. Thus, this standard is not applicable.

Standard 16

In states promulgating the health information provisions of the NAIC model regulation, or providing equivalent protection through other substantially similar laws under the jurisdiction of the Department of Insurance, the Company has policies and procedures in place so that nonpublic personal health information will not be disclosed except as permitted by law, unless a customer or a consumer who is not a customer has authorized the disclosure.

Comments: This standard has a direct insurance statutory requirement relating to HIPAA and requires authorization for the disclosure of patient information. Also, Pennsylvania Insurance Department guidelines clearly state: "Authorization is not required if the disclosed health information is usual, appropriate or acceptable for the purpose of performing one of the 32 insurance functions outlined in the regulation. Examples are claims administration, underwriting, ratemaking and fraud detection and prevention."

Results: Pass

Observations: As asserted by the President, few patient records (non-public personal health information) are handled or maintained by the JUA. Employees are informed of the proper handling of personal information as required by HIPAA regulations, and are required to sign confidentiality agreements as well.

Recommendations: None.

Standard 17

Each licensee shall implement a comprehensive written information security program for the protection of nonpublic customer information.

Comments: This standard has a direct insurance statutory requirement relating to HIPAA as it relates to claim information and requires that the JUA operate under an information security program that is designed to:

(1) Ensure the security and confidentiality of patient information included in claims;
(2) Protect against any anticipated threats or hazards to the security or integrity of the information; and
(3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.

Results: Fail.

Observations: Employees are informed of the proper handling of personal health information, related to claims, as required by HIPAA regulations, and are required to sign confidentiality agreements as well. However, there is no written information security program and no public statement addressing the handling of "nonpublic customer information". Furthermore, lax physical security presents the risk that personal healthcare information related to claimant files, both hard copy and electronic files could be stolen or accessed without appropriate authorization.

Recommendations: An internal security policy should be drafted and approved by Management and the Board of Directors. It should address the following topics:

- How the organization ensures the security and confidentiality of customer and claimant information,
- How it protects against any anticipated threats or hazards to the security or integrity of the information, and
- Identify safeguards to prevent against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer or claimant.

Finally, management should consider adding a statement to the JUA website discussing JUA's concern for the proper and private handling of policyholder and claimant information.

2 (a) - Underwriting Practices and Procedures

Primary Professional Liability policies issued by the JUA are currently subject to a maximum liability limit of $500,000 per occurrence and $1,500,000 per annual aggregate. In addition to the primary coverage provided by the JUA, health care providers must obtain excess professional liability coverage of $500,000 each occurrence and $1,500,000 per annual aggregate provided by the Medical Care Availability and Reduction of Error Fund ("Mcare") by paying a certain percentage of the prevailing primary premium charged by the JUA. The appropriate percentage ("assessment") varies each year based upon payments made by Mcare in the previous year.

The JUA had approximately 1,740 policies inforce at the end of March 2005 compared to approximately 2,094 in-force policies at the end of March 2004. Management estimates that approximately 35% of new and renewal policies are processed during the three-month period prior to December 31, while approximately 15% of the JUA's new and renewal policies are processed during the three-month period prior to June 30 of each year.

Two experienced professional liability underwriters process the current policy business. Exceptions to underwriting that require referral to the President with appropriate recommendations have been clearly documented. Two full-time employees have been trained to assist with underwriting functions. Underwriting functions include reviewing applications for insurance; requesting answers to unanswered application questions; reviewing prior loss history, if any; verifying status of professional license; verifying classification; and related activities to match risk exposure with the correct rate. One of the underwriters also maintains the Mcare database and subsequent premium payments.

During peak periods, the underwriting staff functions near, but not at full capacity. Depending on the extent of an unexpected surge in new applications for insurance beyond present levels, the underwriting department could need to expand quickly to function effectively. Management is aware of the potential need to add underwriting staff if events beyond its control cause an inordinate inflow of new applications. It is also experienced in doing so from recent JUA history. Further, Management believes that, given its personal industry contacts and the desirable physical location of the JUA, hiring and training additional underwriting staff would not be unduly burdensome to gear up quickly for a significant surge in sustained volume.

2 (b) - Claim Handling Practices and Procedures

The JUA employs a full-time Claims Manager to initially screen newly reported notices of claim incidents and to verify insurance coverage with the JUA.

Since January 1, 2003, the JUA has retained the services of Pinnacle Risk Management (Pinnacle) to provide claim-handling services at a predetermined cost for each new file assignment. Most claims reported after January 1, 2003 are assigned to Pinnacle for claim handling purposes. Approximately 150 claims have been assigned to Pinnacle since January 1, 2003. There are approximately 112 active open claim files as of April 2005. The JUA has on-line access to all claims that are handled by Pinnacle and maintains a hard copy of each claim at the JUA's office.

Claim handling services performed by Pinnacle include claim identification, adjusting and verifying legal expenses incurred in the claim adjusting process. Since nearly all of the JUA's medical liability claims are in litigation, highly regarded outside legal counsel is retained to defend the interests of the JUA and policyholders. The JUA's Claims Manager approves outside legal counsel retained by Pinnacle and reviews loss and loss adjusting reserves recommended by legal counsel and Pinnacle. Pinnacle has the authority to issue claim settlement checks up to $10,000. Checks for amounts greater than $5,000 require the approval of a JUA Board member. The JUA's Claims Manager handles claims not assigned to Pinnacle.

3 - Evaluation of internal control structures relating to claims management and policy issuance.

General Overview of Internal Controls

Internal controls are a crucial element of ensuring that an entity achieves its profitability goals and mission with minimal surprises. Effective internal controls enable management to deal optimally with rapidly changing economic and competitive environments, shifting customer demands and priorities, and restructuring for future growth. Internal controls accomplish these goals by promoting efficiency, reducing risk of asset loss, and helping to ensure the reliability of the financial statements as well as compliance with laws and regulations.

Broadly defined, internal control is a process, affected by an entity's board of directors, management and other personnel, designed to promote reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with applicable laws and regulations.

Effectiveness and efficiency of operations addresses an entity's basic business objectives, including profitability goals and the safeguarding of resources. Reliability of financial reporting addresses the need for an entity to disclose accurate financial

statements including interim reports and financial data derived from such statements. Compliance with applicable laws and regulations ensures the viability of the entity as well as protecting it from legal and reputation risk. Although each is a distinct category, it is important to realize that there are overlaps in the categories when addressing certain needs.

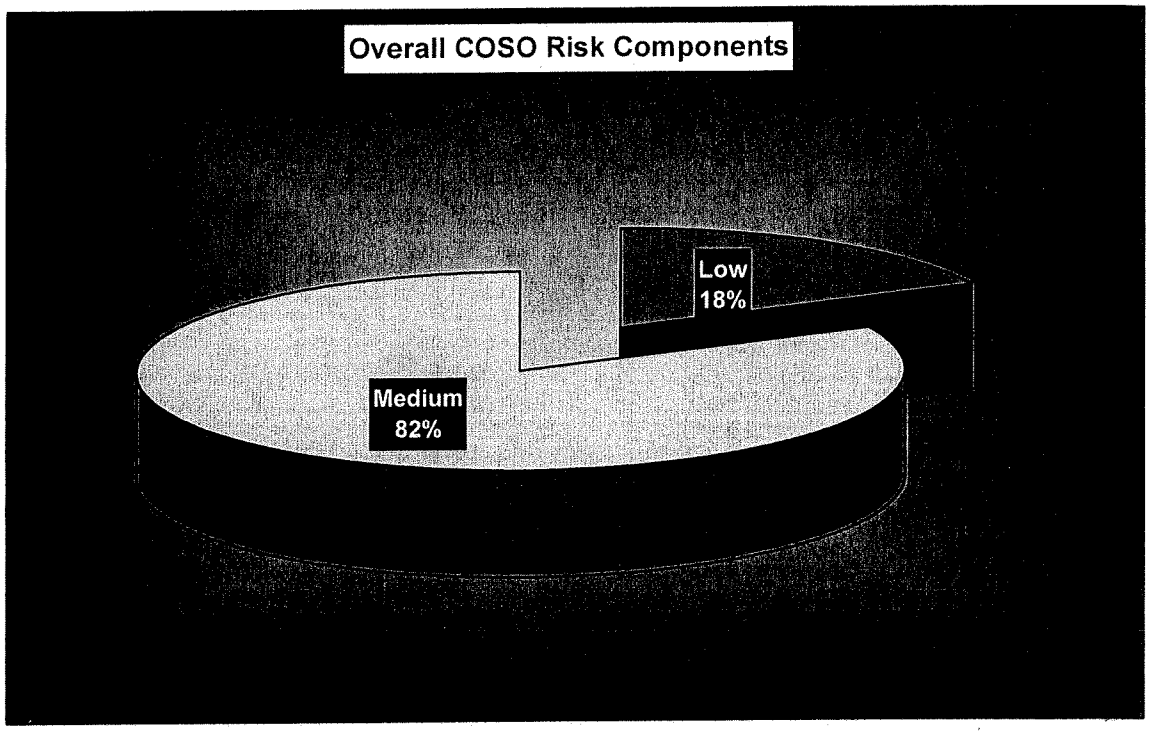
The three elements of internal control consist of five interrelated components. These are derived from the way the business is managed, and therefore should be integrated into the management process. The five internal control components are as follows:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

There should be a synergy and direct relationship between these five components. All of these components together should form an integrated system that reacts dynamically to changing conditions. Internal controls are most effective when they are part of the infrastructure of an enterprise. Such "built-in" controls support the organization, avoid unnecessary costs and enable quick responses to changing conditions.

The following table and graph present our assessment of the JUA's internal control structure:

COSO Internal Control Components	Assigned Risk
Control Environment—Integrity and Ethical Values	Medium
Control Environment—Commitment to Competence	Low
Control Environment—Board of Directors and/or Audit Committee	Medium
Control Environment—Management's Philosophy	Medium
Control Environment—Organizational Structure	Medium
Control Environment—Assignment of Authority and Responsibility	Medium
Control Environment—Human Resources Policies and Practices	Low
Risk Assessment	Medium
Control Activities	Medium
Information and Communication	Medium
Monitoring	Medium



Concluding Comments

The current professional liability market in Pennsylvania appears to be stable. Existing carriers that are licensed or approved to write medical liability insurance coverage have expanded and are absorbing new health care accounts and writing higher volumes of premium income in recent years. Consequently, the JUA has recorded a decrease in new business submissions. Nonetheless, long-standing challenges for the JUA are difficult and require professional attention to be prepared for market forces beyond their control. Sooner or later the market cycle will turn.

The JUA has established and implemented efficient systems and procedures to assure that all health care providers within the Commonwealth of Pennsylvania have access to affordable professional liability insurance. Longer term, uncertainty abounds in the medical liability insurance market. If it happens that medical professional liability rates do not continue to increase gradually to keep pace with increasing exposures associated with professional liabilities, adverse underwriting experience will force insurers to cut back inforce policyholders or pull out of the professional liability market entirely. In that event, the JUA, as presently organized, may need to make certain adjustments to meet its statutory mandate. Historically, Management has made major adjustments to changing conditions.

Findings (other than from market conduct standards evaluated and presented above) are attached to this report.

INS Services, Inc.

By: _____
Lawrence R. Lentini, CPA
President

High Risk Findings

The following exceptions must be addressed by the JUA:

Physical Security

Finding:

Physical security is lacking. Three external office doors remain unlocked and essentially unmonitored during business hours (8:00 AM to 4:30 PM). Occasionally, doors may remain unlocked and unmonitored even beyond business hours. The servers reside in public office space, accessible by all employees and visitors. Within this space, there are no environmental alarms to alert management of high temperatures during non-business hours. Tapes are kept on a shelf in full view. An Uninterrupted Power Supply (UPS) device is in place but no automated server shutdown has been configured to prevent data loss in the event of a power outage.

Recommendation:

Information Security has not been formally addressed in any of the JUA manuals. We recommend that a security policy be drafted by Management and approved by the Board of Directors.

Specifically, the following items relate to physical security.

- Office doors should be locked to prohibit access from the shared hallways and the front door should be locked when no receptionist is present.
- The servers should be kept in locked office space.
- Access to workstations as well as the server should be limited through the use of password protected screen savers.
- Servers should reside in a space with adequate ventilation, fire detection and temperature monitoring (at minimum a recording thermometer), as excessively high temperatures may cause hardware damage.
- In the event that systems must be shut down there should be written procedures posted near the server. While the management team and lead administrative assistant know how to shut down the server, posted written procedures would benefit anyone else called to do so in an emergency.

If at all possible, the UPS should be configured to shut down the server (through the use of a batch file) in the event of a power failure. This would be especially relevant to "after hours" automatic procedures such as tape back-up. To prevent data loss, UPS should be connected and configured to terminate all programs and initiate a controlled server shutdown prior to backup battery power depletion.

Company Risk:

The preceding items relate to fire, theft or employee sabotage, all of which must be considered in assessing the risks of inadequate physical security. Physical exposures could result in financial loss, legal repercussions, or loss of reputation.

Employee Screening

Finding:

During an interview, the President disclosed that background checks for new hires include reference checks from candidates' prior employers and other business references. The JUA does not verify education, salary, job and credit histories; and, criminal conviction and driving records.

All organizations should have pre-employment screening procedures designed to eliminate the risk of hiring employees with a history of fraudulent or criminal behavior. Under 18 U.S.C. §1033, the JUA is required to report criminal actions to the Department.

Recommendation:

We recommend the JUA perform criminal background checks of all employees.

Ideally, background screening should also include verifying education, salary, job-title and credit histories; and, driving record. Given the relatively small number of employees and their job descriptions, the JUA should consider which of these recommendations bests fits its needs, considering risk, derived benefits and cost.

Company Risk:

Inadequate pre-employment screening increases the risk of hiring employees with a history of fraudulent or criminal behavior. Failing to adequately screen employees may expose the JUA to liability.

Audit Committee Participation

Finding:

During interviews with the President, it was disclosed that an Audit Committee has existed and met on occasion, but there is no formal charter to establish its responsibilities. The "Pennsylvania Professional Liability Joint Underwriting Association Amended and Restated Plan of Operations" (March 2005) does not define an audit committee as part of the board.

Recommendation:

It is constructive to take a "fresh look" at the internal control system from time to time, focusing directly on system effectiveness. The scope and frequency of separate evaluations will depend primarily on an assessment of risks, and ongoing monitoring procedures.

While the vertical structure of the organization ensures that senior management and the board are informed of deficiencies when they are recognized, it appears that the deficiencies could exist for a period of time (between annual audits) without being detected. Due to the size of the organization, an internal audit function is neither practical nor recommended. However, a formal Audit Committee charter should be established.

The responsibilities of the Audit Committee should include:

- Selection of the audit firm and its terms of engagement
- Defining and assessing the work and responsibilities performed monthly by the outside accountant. For example, the role of the outside accountant could be defined by the Audit Committee so that the accountant could act as a supervisory control through the review and sample testing of underlying data, reconciliation of such data to accounting records, and analytical procedures. Smaller entities subject to outside scrutiny frequently take this approach to improve internal controls, especially the element related to monitoring.
- Creation of a logical and practical methodology for periodically evaluating system controls.

Company Risk:

Many of the risks that could result in losses to an organization are within operational areas. Without a well-balanced and effective risk assessment plan, there is no assurance that risks are identified and evaluated as part of an ongoing risk assessment process, or that the JUA's risk response (including the design and application of its internal controls) to identified risks are adequate to mitigate those risks.

<u>Logical Security</u>

Finding:

Critical database access controls are ineffective, and may result in data theft, loss or corruption. The Microsoft Access databases are not designed or configured to limit appropriate data rights for each user by role and responsibility. Presently, logging of changes to the database or its code is nearly impossible.

Also, prevention or detection controls over database code modification (data formatting, indices etc.) are not in place, thereby affecting existing controls.

Microsoft Access is not a scalable solution. Microsoft recommends that the scalability path for Access is to migrate to Microsoft SQL.

Data stored in Microsoft Access poses serious security risks. Organizations dedicated to widely accepted compliance standards must identify all sensitive data stored in Microsoft Access databases and then secure it from unauthorized access. Even the most secure Access databases (those that employ user-level security and encryption) are easily penetrated using inexpensive cracking tools.

Management stated that the JUA stored data is not sensitive because it does not include personal, credit or patient information. The only JUA sensitive data is the financial data stored in Great Plains Accounting software. Great Plains Accounting runs on Microsoft SQL, so we can conclude that the JUA server is capable of supporting other SQL databases.

Recommendation:

Given its size and business volume, JUA requires its employees to perform numerous and shared functions. Consequently, it may not be practical to limit users to defined roles and limited access. However, we recommend that Management consider ways to improve supervisory controls within reason to assure that database field changes can be detected and reviewed by Management, and that only Management can authorize changes to user rights.

Security enhancements will require code changes to each database, and user access changes each time roles change. While this can be accomplished in Microsoft Access, the cost and development effort may be equal to that of migrating data to a more robust database platform, such as Microsoft SQL, Oracle or MySQL. The conversion to one of these secure DBMS platforms can be performed while preserving the user interface and program operation, thereby minimizing redevelopment and training costs.

Ideally, the following controls should be present for databases such as SQL, Oracle or MySQL:

- Definition standards to ensure accuracy, completeness and consistency of data elements and relationships within the database.
- Access controls for data items, tables and files to prevent inadvertent or unauthorized access and/or modification.
- Controls to handle concurrent access problems, such as multiple users performing updates simultaneously.
- Accurate and complete backup and restoration of data, in a timely manner.

- Incorporate event logging and tools to monitor the integrity of the data and to track any unauthorized access.

We suggest that JUA issue a Request For Proposal to upgrade to SQL, and then perform a cost benefit analysis.

Company Risk:

Inadequate controls over critical database applications could increase the likelihood of errors as well as unintentional or intentional unauthorized access, and/or modification to programs and/or data. Also, database availability is most important to business operations, and poor application design may result in downtime and inefficient use of technological and human resources. However, supervisory controls performed by Management and monthly review of data by the outside accountant somewhat mitigate these internal control risks for JUA.

Documentation of Controls

Finding:

While Management has stated, "All processes are reviewed regularly to see that they are working," these regular reviews are not documented. In smaller entities like the JUA, such reviews often exist but without formal documentation.

Recommendation:

Rather than documenting each and every review step, perhaps a checklist of required reviews and reconciliations could be prepared and then initialed after each step is performed. Further, as mentioned previously, the Audit Committee could assign monthly supervisory control procedures to the outside accountant. Reporting by exception, the accountant could communicate monthly to Management and the Audit Committee.

Company Risk:

Not documenting a control step does not necessarily mean the control was not performed. However, it would be prudent to document certain control procedures to enhance accountability, accuracy and diligence since undocumented procedures could eventually lead to inadequate or incomplete control procedures and complacency. Further, the possibility of errors increases when new employees or changing responsibilities enter the process. In such an environment, errors could occur if the control step is not performed.

Disaster Recovery Procedures

Finding:

No formal disaster recovery or business resumption plan exists. Tape backup and restoration procedures are not formally documented and there are no manual checklists to ensure that tapes are changed as required by a documented backup schedule. The monthly or yearly tape cycles and tape rotations are not documented. Onsite tape storage is insecure (tapes are kept on a shelf in full view of employees and visitors). Management taking the tapes home at night achieves off-site tape storage, but there is no inventory list to locate tapes when needed.

Although management has successfully relied on a computer services firm that is conveniently located in the same building, this could pose additional risks in the event that the building is damaged, since that firm's operations may also be impacted.

Recommendation:

We recommend that management, in conjunction with the computer support vendor or vendors, create a comprehensive disaster recovery/business resumption plan. Contingency planning for the loss of all data systems will drive the analysis of what is needed to restore operations from "scratch." The plan should detail day-to-day procedures for backup and the steps required for recovering any files, application or the entire operating system. The analysis will include a discussion of the risks of various tape rotation strategies. For example, is it possible to re-enter daily data if only data from the prior evening or second prior evening can be recovered from tape?

Other items that should be included in the plan are:

- An up to date list (revised periodically) of all emergency contacts within the organization as well as vendors who may be required to assist in recovery efforts.
- Step by step instructions for the recovery team.
- A prioritized list of applications and sequence for restoration.
- Required manual procedures performed by employees until computer systems are restored.
- A list of all computer hardware so that replacement hardware is compatible with existing systems – this list should be updated whenever system changes occur.
- Administrative account and passwords required for data and system recovery.
- Multiple copies of the plan stored on and off-site in convenient but secure locations.

- The plan will include a testing schedule and test procedures. Testing should take place annually and the results should assure management that disaster recovery procedures work.

To ensure that recovery plans are successful, daily tape operations should include a log or checklist confirming that scheduled backups are complete. Errors should be noted and backups should be re-run according to established procedures to ensure that *all data* can be restored. We also recommend that as part of daily operations, a tape inventory be maintained. On-site tapes not residing in the tape drive should be stored in a locked cabinet or preferably in a small, dedicated fireproof safe. A simple form can be used so that tapes are logged by date and labeled each time they are replaced or moved to off-site storage.

While taking tapes home at night may be adequate protection, a special archive service (such as Iron Mountain, which JUA currently uses for paper archives) should be considered, if not cost prohibitive, as this ensures that tapes are kept in an environmentally secure location that can be accessed at any time of day. However, if the cost exceeds the benefit, a two-day backup may provide a reasonable alternative. For example, a backup could be performed on Monday and held by one manager off-site until Wednesday. Another backup could be performed on Tuesday and held by another manager until Thursday. This approach reflects the unlikely scenario that data held at three different locations would be lost simultaneously.

Further, at least quarterly, a full backup set reconciled to the accounting records should be maintained off-site for business archives as well as disaster recovery.

Company Risk:

Natural and man-made hazards can expose the JUA to loss of data as well as operational downtime. Without well-designed and routinely tested backup and recovery procedures, unpredictable events may result in extended operational downtime.

Moderate Risk Findings

The following exceptions should be addressed by the JUA:

Major Outsourcing Relationships

Finding:

The JUA does not have a formally documented vendor selection process for significant outsourced functions, or standards for drafting contracts or service

agreements with significant or material (see our discussion of materiality below) vendors and the administration of such relationships.

The JUA was able to provide evidence of formal agreements with Pinnacle (claims), Fair Plan (data storage), Deutsche Asset Management (investments), Princeton Financial Services (investment advisor), Wachovia Bank (trusts) and Pricewaterhouse Coopers (auditors).

While the JUA was able to produce a copy of the Pinnacle Service Agreement identifying the responsibilities of the JUA and the vendor, the contract upon which this Service Agreement was drafted was not available for review. Pinnacle is the only new vendor to whom services have been outsourced in recent years. The Board of Directors delegated approval to the Claims Committee; however, the Claims Committee does not maintain minutes from meetings.

With the exception of Pinnacle, Wachovia, Pricewaterhouse Coopers, LLC and Deutsche Asset Management, the JUA does not have documented warranties with other vendors to whom business services have been outsourced. Neither compliance with warranty requirements, nor vendor performance is monitored for any of the Companies. The JUA recently reviewed claims files at Pinnacle in January 2005; however this is not a regular practice, with that review occurring because JUA personnel were already onsite for another reason. Additionally, security requirements to be adhered to by the vendor are not defined within any of the documentation provided by the JUA.

Recommendation:

The Board should develop standards for vendor selection for material services or products. Materiality should reflect due consideration to not only the amount of the contract, but the impact that disruption, interruption, failure to perform or termination of services could have on the JUA (reference our prior recommendation regarding Audit Committee Participation above i.e., identification of risk events and development of adequate risk responses). Where appropriate, vendor selection standards could also include the following:

- A minimum number of potential vendors for comparison, evaluation and selection.
- Criteria for vendor review.
- Costs and the vendor's ability to perform
- Vendor's understanding of the JUA's needs and reflection of that in the proposal.
- Vendor selection authorization limits.

Once a major vendor is selected, contract language could give consideration to the following standards where appropriate or relevant, and the contract is material:

- Management's requirements and expectations
- Detail of services to be provided
- Quantitative and qualitative service level agreements
- Costs of services
- Payment requirements and frequencies
- Problem resolution processes
- Penalties for non-performance
- Dissolution processes
- Agreement modification processes
- Reports processed, including content, distribution and frequency
- Roles and responsibilities of principals
- Duration of contract
- Appropriate access levels (by the JUA to vendor systems and by the vendor to JUA systems)
- Security requirements
- System maintenance and technical support
- Non-disclosure agreements
- Audit rights

The JUA should define and document those circumstances requiring legal counsel to review and/or the Board to approve significant contracts.

Company Risk:

Inadequate policies and guidelines for the review and selection of major vendors could hinder the JUA's ability to select the contractor best suited to its business needs. The absence of approved contracts for material outsourced functions could potentially result in a misunderstanding of roles and responsibilities, added costs, and an interruption in business operations.

Periodic Risk Assessment

Finding:

Management's response to several audit questions suggest that changes have been made in response to sudden business needs. Historically, these responses have proven successful, but proactive contingency planning should eliminate the need for reactive responses. Management has stated that frequent contingency planning discussions are held between management and the Board as well as with staff, but records do not evidence periodic reevaluation.

Recommendation:

Formal risk assessments should be documented as such and updated periodically. This may take the form of an annual or other periodic risk assessment, which should include minutes of risk assessment meetings. The risk assessment should identify and evaluate specific risks.

Contingency plans should be refined and updated accordingly. For example, lists of vendors and staffing agencies should be updated and new sources of information should be compiled on a periodic basis, or as new information becomes available. Information systems contingency plans should include restoration of data and hardware.

Company Risk:

Contingency plans that are no longer current may not provide viable solutions when changes or confusion occur.

Unless risk assessment is conducted periodically and documented, existing controls may not adequately protect the organization from continually changing operating conditions. Documenting the decision process leads to a dynamic process for improvement.

Office Asset Management

Finding:

During the interview process, management stated that there is no asset inventory available. While there may be lists or records of equipment and software purchases, they could not be assembled, as may be required in the event of loss, theft or questions of proper licensing (software in particular).

Recommendation:

An asset inventory should be maintained, particularly in respect to data systems, as they contain valuable JUA information. From a disaster recovery perspective, the asset inventory would be needed to ensure that compatible hardware is used to facilitate the restoration of critical systems.

The asset inventory should be kept current and include the following at a minimum:

- A list of all office equipment and furniture.
- Telecommunications equipment and specifications.
- Computer hardware including number of units, purchase price, date, vendor, model and configuration.

- Computer software - preceding plus the version, license numbers and license period, where applicable.

Company Risk:

Assets should be tracked to properly assess loss from theft, vandalism and environmental damage. Software assets must be tracked to prevent liability from software licensing violations as well as to ensure that software is upgraded in a timely manner.

Pennsylvania Professional Liability Joint Underwriting Association

PLYMOUTH WOODS
521 PLYMOUTH ROAD, SUITE 101
PLYMOUTH MEETING, PA 19462-1638

PHONE (610) 828 - 8890
FAX (610) 825 – 0688
Email: Insurance@PAJUA.com

Thursday, September 15, 2005

Mr. Chester Derk
Market Conduct Division Chief
Bureau of Enforcement
Commonwealth of Pennsylvania
Insurance Department
Room 1321 Strawberry Square
Harrisburg, PA 17120

Re: Market Conduct Exam

Dear Mr. Derk:

Please accept this in response to the Market Conduct Exam letter dated August 16, 2005. To avoid duplication in the responses, the items in the letter addressed to Mr. Shoop are addressed together with the risk findings in the second section of the letter.

We wish to take this opportunity to thank the department and the staff of Ins Services, Inc. for the way in which the examination was handled. The input we received was helpful and has given us some insight into areas where our operation can be improved.

Sincerely,

Susan M. Sersha

Susan M. Sersha

cc. Henry O. Schramm, II, Audit Committee Chairperson

Letter to Dennis Shoop dated April 7th 2005

Standard 2:

See Physical Security

Standard 3:

See Employee Screening

Standard 4:

See Disaster Recovery and the Atlanta and coarsely in the

Standard 10:

See Physical Security And Logical Security

Standard 17:

See Logical And Physical Security

High-risk Findings

Physical Security

The premise is equipped with a fire detection system that protects the server's current location. Temperatures up to 190 degrees would not damage the equipment. Should the temperature exceed 190 degrees the operating system would shut down the system.

If the UPS is running low on power because of an extended power outage, system messages are generated advising everyone currently logged onto the system that shutdown is pending and when it will begin. At the end of that period, the system begins an orderly shutdown.

Several steps have already been taken to increase physical security. A security policy will be drafted for review and modification by the audit committee and, with board approval, implemented.

Employee Screening

We will review employee screening tools including the feasibility of conducting criminal background checks on potential new hires. A company policy will be drafted for review and modification by the audit committee and, with board approval, implemented.

Audit Committee Participation

A formal audit committee charter will be established for review, modification and approval by the board.

Logical Security

Definition standards currently exist for data elements and relationships within the databases. A review of those standards will be conducted to ensure they are current and a regular review scheduled annually or whenever database modifications are made.

Controls to handle concurrent access problems are already in place.

Backup and restoration procedures are in place to ensure data can be restored in a timely manner.

A data management policy will be drafted for review and modification by the audit committee and, with board approval, implemented.

Documentation of Controls

A checklist of required reviews and reconciliation will be developed by management and completed monthly for all month end functions. The outside accountant will review the checklist. Management will review any items completed by the outside accountant. Any exceptions will be reported to management and the audit committee.

Disaster Recovery Procedure

A disaster recovery procedure will be drafted for review and modification by the audit committee and, with board approval, implemented.

All items shown on the list under the recommendations will be considered in developing such a plan.

Moderate Risk Findings

Major Outsourcing Relationships

Standards will be drafted for review and modification by the audit committee and, with board approval, implemented. The standards will consider the items listed under the recommendations.

Periodic Risk Assessment

A formal risk assessment document will be created an updated periodically. The establishment of the appropriate periods for such review and updating will be submitted to the audit committee for confirmation, modification and, with board approval, implemented.

Office Asset Management

A list of the current computer hardware, telephone equipment and newer furniture has been developed and appropriate replacement cost established. Older furniture that would not be replaced if destroyed is not included. Vendor and purchase date will be included for major items such as desktop computers, phone equipment, server and high-speed printers. If the equipment has a serial number, the serial number will be added to the inventory list.

The list will be updated to include version and license numbers for computer software.